[THIRD DRAFT. Comments welcome.] 3/6/02

Legal and Ethical Constraints on Terrorism Prevention Technologies: Slippery Slopes, Balancing Acts, and Constitutional Values

Mariano-Florentino Cuéllar
Stanford Law School

Preventive technology may be a promising means of limiting the threat of terrorism, but its deployment should be scrutinized for consistency with constitutional doctrine and the values underlying that doctrine. The constitutional doctrine prohibits some government uses of preventive technology and sheds light on important values such as privacy protection, but does not definitively resolve questions about the legal and ethical constraints to which preventive technologies should be subjected. This requires attention to the specific characteristics of a deployed technology, including its invasiveness, actual performance, due process protections, and preventive or law enforcement justifications. The most difficult issues in evaluating technology deployment arise when considering the marginal benefits and costs as compared to existing enforcement strategies (a useful but challenging comparison), and addressing the often-invoked but sometimes misunderstood slippery slope problem. While neither the cost-benefit issue or the slippery slope issue is intractable, addressing them implies that different ethical constraints should be imposed on technologies depending on how invasive they are, whom they target, what goal they serve, and how feasible it is to design mechanisms that will restrain the technologies' abuse by government or private entities.

I. INTRODUCTION

The American people experienced two notorious episodes during the mid-20th century that raised the question of how to balance security and civil liberties. One was McCarthyism – a bundle of anti-communist congressional investigations, security concerns, public hysteria, and rhetoric commonly viewed today as having been riddled with excess.[1] The modern-day rejection of McCarthyism stands despite the impression by some commentators and scholars that the U.S. was indeed at some risk of what, for lack of better terms, could be termed "infiltration" by communists.[2] The other episode

[1] *See*, e.g., R. ROVERE, SENATOR JOE MCCARTHY 232 (1959).
[2] *See* Communist Party of the U.S. v. Subversive Activities Control Board, 367 U.S. 1, 54 (1961)(upholding federal agency determination finding a substantial threat of communist infiltration and that communist organization in the U.S. was directly controlled by the Soviet Union); *but see,* e.g., Irving Louis Horowitz, *Culture, Politics, and McCarthyism: A Retrospective From the Trenches*, 22 WM. MITCHELL L. REV. 357 (1996)(expressing some skepticism about the extent of the threat).

was the World War II era reaction to the perceived threat of Japanese Americans on the West Coast who were feared to favor Japan and to pose a risk of sabotage.[3] In both cases, the historical record is one that generally provokes embarrassment today and is used as the basis to question whether concern over security fundamentally places at risk the civil liberties that make the U.S. worth defending.[4]

But McCarthyism and Japanese internment might also be used to tell a different story – a story of how apparently pressing threats led to clumsy enforcement strategies. In both cases, the enforcement strategy was predicated on brute categories meant to serve as a proxy (i.e., having been mentioned by someone else as a possible Communist sympathizer, or being of Japanese descent and living in the West Coast). If the problem was indeed the enforcement strategy, it raises the question of whether society would have been better off if it had technologies available during the 1940s and 1950s that might have been far less clumsy in singling out communist infiltrators and Japanese collaborators (if any existed). Perhaps a database could have analyzed hundreds of millions of pieces of information applying a rational algorithm to classify people on the basis of risk. If they had access to the appropriate technology, investigators might have used a supremely effective lie detecting device calibrated to focus only on the security issues of the day. The more effective the technology, the fewer false positives it would give, and the less likely that a genuine offender would elude detection. The widespread availability of such technology might have exposed the fallacies of clumsier enforcement strategies that punished people because of their ethnic background or their inclusion on a list of dubious validity. Based on what we know in hindsight and assuming the technology worked accurately (admittedly a heroic assumption), the human cost of both McCarthyism and Japanese internment would have been minimized because fewer people would have been interned, blacklisted, suspected, questioned, harassed, or demeaned.

---

[3] WILLIAM H. REHNQUIST, ALL THE LAWS BUT ONE 195-207(1998)(noting that the possibility of sabotage by Japanese Americans on the West Coast could be considered a threat, and that under Japanese law even U.S. born children of Japanese citizens were themselves Japanese citizens); *but see* Hirabayashi v. United States, 828 F.2d 591 (9th Cir. 1987)(dismissing U.S. government's alleged evidence of any threat from Japanese Americans, and vacating an internee's conviction because of "manifest injustice" in the government's prosecution of the original case). *See generally* Eugene V. Rostow, *The Japanese American Cases – A Disaster*, 54 YALE L.J. 489 (1945); Nanette Dembitz, *Racial Discrimination and the Military Judgment: The Supreme Court's Korematsu and Endo Decisions*, 45 COLUM. L. REV. 175 (1945).

[4] Rovere, *supra*; Rostow, *supra*.

Among some of us the hypothetical scenario makes George Orwell look tame, and inspires as much alarm as the actual occurrence of McCarthyism and Japanese internment -- if not more. The question is why. Is it because we would not trust the government to use such technology responsibly? Or is it because the use of such technology – even for laudable purposes and subject to fail-safe protections against government misuse – would violate constitutional law, or perhaps even the values and principles animating the law? These are the questions that animate this paper, only the context is not some imagined reenactment of McCarthyism or Japanese internment but the here and now of live terrorist threats and lively, increasingly advanced technologies – many of which provoke intense controversy.[5] Its goal is to make an initial effort to understand the proper role of legal and ethical constraints on the promising technologies discussed here that would help reduce terrorism's threat.

The starting point for that framework is the Constitution, because the deployment of technology should comport with constitutional doctrine in the areas most directly related to that deployment, including Fourth Amendment doctrine, other privacy-related constitutional doctrines, free speech and association doctrines, and due process. The question is then what other constraints should apply to the deployment of technology, which could be implemented through statutes or other policies. My argument is that the Constitution itself – despite the blemishes in its own history and in our interpretation of it – is a fertile source of principles to develop those constraints. These "constitutional values" are ones reflected in some of the relevant doctrines and include the importance of balancing costs and benefits, the inherent value of privacy, and the importance of some form of due process. What all of this reveals is as simple as it is important. The Constitution does provide doctrines constraining government use of some preventive technologies, particularly involving home surveillance and highly intrusive criminal investigation of suspects using unusual technologies. But there is a need for further legal

[5] American Civil Liberties Union, *Safe and Free in Times of Crisis*, at http://www.aclu.org/safeandfree/index.html (January 24, 2002)(highlighting specific concerns about privacy and technology).

and ethical constraints to protect constitutional values, as some preventive or law enforcement strategies may be constitutional but not wise.[6]

I consider the nature of those constitutional values in Section II, then analyze (in Section III) the major applications of preventive technology discussed in the conference in light of the constitutional values. The survey of technologies highlights the two most pervasive problems (discussed in Section IV) in developing legal and ethical constraints: balancing costs and benefits, and managing the so-called slippery slope. As the conclusion (Section V) notes, both are vexing problems -- yet they can be partially addressed through a variety of legal and political strategies. Perhaps these strategies can make preventive technology a vehicle to promote security and also to reduce the incidence of clumsy, overbroad enforcement reminiscent of McCarthyism and Japanese internment – without making Orwell turn in his grave.

II. CONSTITUTIONAL LAW AND CONSTITUTIONAL VALUES

No reasonable person can argue away the profound threat of terrorism, which might be usefully defined as the deliberate imposition of violence on civilians to achieve political objectives. Even if we have sometimes failed to grasp the magnitude of that threat, it is a threat that has effectively grasped us. Even if the September 11 death toll is a small proportion of the national murder rate or the daily death toll from traffic accidents, there is something particularly insidious about terrorism's threat. Traffic accidents somehow seem "natural" occurrences when compared to deliberate mass killings of civilians, and individual murders seem to pale in comparison to reasoned efforts made to maximize death and harm.

The deployment of technology to prevent terrorism is useful because it advances preventive and law enforcement missions, and has the potential to prevent abuses associated with existing law enforcement strategies.[7] But the use of technology should be

---

[6] For example, private sector organizations are not subject to constitutional regulation but they can also abuse preventive technologies, which is why many existing statutes focus on what the private sector does with information. *See* discussion on private sector constraints, in Section II., *infra*.

[7] *See* Sections III and IV for a discussion of how the deployment of technology can prevent abuses associated with existing law enforcement strategies.

subject to legal and ethical constraints embodied in the Constitution.[8] Because judicial[9] and even legislative[10] interpretation mediates the impact of the Constitution, it is worth considering constitutional doctrine to understand what sorts of enforcement strategies might be constitutionally suspect. Accordingly, the discussion that follows serves a dual purpose: to review the relevant constitutional constraints that might exist on enforcement strategies, and also to highlight the constitutional values that should inform debates about what ethical constraints to enact through statutes or policy prescriptions.

Because technologies differ so much in the substance of what they do and what goals they serve, my goal here is to describe a few principles that are most useful in fashioning ethical constraints for preventive technology deployment, and legal (i.e., statutory or policy) constraints based on the ethical ones. My analysis depends on three premises. First, technologies are different from each other. Obviously sensor and data collection technologies are different from each other, but so too are different kinds of technologies within the same grouping – such as sensors that pick up voice communications compared to those that detect explosives. Second, interested parties have different objectives and degrees of power to influence outcomes. For example, legislators may try to specify exactly how a technology will be used but may not always succeed. If legislators want to control the execution of technology deployment they will tend to use the resources at their disposal (i.e., budgets and lawmaking) to achieve their particular objectives; so too will other actors in the system, including regulators, investigators, prosecutors – and terrorists. Finally, enforcement strategies can be substitutes for each other. Thus, if budget constraints prevented airports from implementing explosive detection sensors, airport screeners and law enforcement

---

[8] Statutory constraints are best viewed as a reflection of – rather than a definitive guide to – ethical constraints, since they are constantly subject to change. Some statutes, though, are difficult to change as they are buttressed by super-majoritarian institutions *See generally* KIETH KREHBIEL, PIVOTAL POLITICS: A THEORY OF U.S. LAWMAKING (1998). Note that the same dynamic that makes existing statutes difficult to change also makes it difficult to pass legislation in the first place.

[9] *See generally* Jed Rubenfeld, *Reading the Constitution as Spoken*, 104 YALE L.J. 1119 (1995)("How can a 200 year-old text like the Constitution be interpreted…? In a variety of ways, as we shall see shortly…"); John Hart Ely, DEMOCRACY AND DISTRUST: A THEORY OF JUDICIAL REVIEW (1980)(offering a process-based theory of constitutional interpretation and judicial review).

[10] *See* Elizabeth Garrett and Adrian Vermeule, *Institutional Design of a Thayerian Congress*, 50 DUKE L.J. 1277 (2001)(describing the importance, and frequency, of Congress' constitutional interpretation).

personnel would not stop searching for explosives – they would simply use other strategies to do so.

I leave for another day the question of what specific institutional arrangements are best suited to impose and fill in the details of the legal and ethical constraints. My focus instead is first on principles that would assist any institution (or even members of the public) in deciding on the appropriate constraints. My concern is less with who should apply these principles than with trying to articulate a few of them that will guide deliberations of a host of important audiences, including policymakers, regulators, the law enforcement community, and public deliberation and discussion.

A. Privacy and Police Power: Fourth Amendment Doctrine

The Fourth Amendment regulates how and when the police engage in a search or seizure of a person or property.[11] A full discussion of Fourth Amendment doctrine is beyond this paper's scope. Nonetheless, two things about this doctrine are especially relevant to our inquiry. The first is that the doctrine evinces a concern (or at least an attempt to be concerned) with privacy – a concern reflected partly in how the Supreme Court has sought to limit some police uses of technology to gather evidence against suspects. The second point is that the doctrine does draw some distinction between police activity that is primarily aimed at gathering evidence for a suspect's trial, and regulatory or national security-related activities that in principle focus on preventive functions.

Consider first how the doctrine works in the situations to which it is most applied: police investigations. In the idealized law enforcement investigation, a police officer obtains a warrant before undertaking a search or a seizure, to establish the existence of probable cause.[12] If a search is not conducted with a warrant, the search must be reasonable if police officers want to use evidence against the suspect.[13] But this begs the

---

[11] U.S. CONST., FOURTH AMENDMENT.

[12] *See* Kyllo v. United States, 121 S.Ct. 2028 (2001)(noting in passing the doctrine that "warrantless searches are presumptively unconstitutional")(dicta).

[13] *See*, e.g., Wong Sun v. United States (1963)(concluding that requirements for issuance of warrants and for warrantless searches must both demand a threshold of probable cause, because the requirement for warrantless searches "surely cannot be less stringent" than requirement for issuance of a warrant). The Supreme Court has created categories of wrrantless searches that could be understood to be exceptions to the warrant requirement. *See* William J. Stuntz, *Warrants and Fourth Amendment Remedies*, xx VA. L.

question of what counts as a search. In strictly legal terms, the most direct impact of Fourth Amendment law is on searches made by police officers gathering evidence about criminal activity. Since the early 1960s, courts focusing on police investigation have resolved the question of whether a particular law enforcement strategy is a search by asking whether it violates a person's reasonable expectation of privacy.[14] The doctrine did not always focus on privacy expectations. Instead, courts initially took the "is this a search" question quite literally, focusing on common law trespass doctrine not recognizing that some activities that were not searches in the literal sense of inspecting someone's home could nevertheless amount to a search.[15] Later, the courts recognized that a law enforcement strategy's intrusiveness could help determine the extent to which it should be counted as a search, before finally recognizing that individual expectations of privacy should be a guide to whether a procedure is a search.[16] The most commonly formulated approach to the privacy expectation question inquires first whether a person has a subjective expectation of privacy, and second whether it is an expectation that society is prepared to recognize as reasonable.[17]

The focus on the reasonableness of privacy expectations arises in part from the Supreme Court's broad retreat over the years from a conception of the Fourth Amendment that focus on the protection of property. The trend away from a property-protecting conception of the Fourth (and Fifth) Amendment is underscored by the Supreme Court's relative abandonment of the idea that documentary information should be considered private and testimonial.[18] Although such a doctrine has never been explicitly overruled in the courts, it's been subjected to so many exceptions that it's been effectively rendered irrelevant.[19] This makes records that have been made available to

---

REV. xx (1991). But these exceptions are so routinely useful to law enforcement that the exceptions seem to have swallowed up the rule.

[14] *See* Katz v. United States, 389 U.S. 347 (1967).

[15] *See* Olmstead v. United States, 277 U.S. 438, 464-466 (1928); Goldman v. United States, 316 U.S. 129, 134-36 (1942).

[16] *Compare* Silverman, 365 U.S. at 510-512 (focusing on the invasiveness of an "actual intrusion into a constitutionally protected area") *with* Katz, 389 U.S. at 353 (focusing on justifiable reliance on a reasonable expectation of privacy).

[17] *See* Katz, 389 U.S. at 361 (Harlan, J., concurring); California v. Ciraolo, 476 U.S. 207, 213 (1986).

[18] *See* Boyd v. United States, 116 U.S. 616 (1886)(holding that a government subpoena for accused's papers and records violated the Fourth and Fifth Amendments).

[19] *See* Note, *The Life and Times of Boyd v. United States* (1886-1976), 76 MICH. L. REV. 184, 188 (1977)("The *Boyd* majority had to reconcile its doctrine with traditional practices").

private institutions fair game for the government to obtain, at least where there is some broad policy rationale underlying the legislative authorization for law enforcement authorities to examine records.[20] In principle, this allows data collection and analysis technology to churn information obtained by the government, including records collected pursuant to legitimate record-keeping requirements.[21] Individuals targeted because of data collection and evaluation could be investigated further -- but not necessarily seized or searched -- without additional information.

A similar trend toward permissiveness of law enforcement searches is apparent in cases involving the use of investigative strategies or technologies that enhance the human senses. For example, the Supreme Court has held that the use of a so-called "pen" register to obtain the phone numbers a person has dialed does not constitute a search.[22] Neither does the use of a drug sniffing canine at an airport, where the dog is trained to recognize only narcotics,[23] or the use of enhanced aerial photography on an industrial facility.[24] In most cases, the use of sensor and screening technology might fairly be analogized to the drug-sniffing dog or the aerial photography: all involve some means of enhancing the natural senses to gather specific information in the public domain about individuals (or locations).

---

[20] U.S. v. Miller, 425 U.S. 435 (1976)(concluding that a bank depositor "takes the risk, in revealing his affairs to [a bank]," that the information will be conveyed by the bank to law enforcement, and thus has no Fourth Amendment protection against such transfer). The holding clears most Fourth Amendment obstacles to data collection and evaluation. For example, the Treasury Department's Financial Crimes Enforcement Network subjects large currency transactions to profiling analysis (though the system currently does not examine non-currency transactions).

[21] Hale v. Henkel, 201 U.S. 43 (1906)(holding, among other things, that while the Fourth Amendment does not require a showing of some factual foundation for a subpoena, it does prohibit a subpoena duces tecum too sweeping "to be regarded as reasonable"). The Supreme Court here again reveals its penchant for reasonableness and balancing analysis as a means of splitting the difference between distinct conceptions of Fourth Amendment doctrine.

[22] *See* Smith v. Maryland, 442 U.S. 735 (1979). The Supreme Court here upheld a number of surveillance practices on the questionable ground that no justified reasonable expectation of privacy was infringed since had already been revealed in a limited way to a limited group for a limited purpose. If the information revealed and its audience was obviously limited by defendant, it's hard to argue that the defendant would have been indifferent between such limited sharing and complete disclosure. What seems to animate decisions like Smith is the courts' reluctance to recognize gradations in privacy expectations (which are surely pervasive) and instead an interest in making an explicit decision between what is considered private and publicly disclosed. In contrast, an attempt to make gradations between degrees of privacy expectations is not only difficult to undertake because of the complicated inquiry into a defendant's subjective state, but would also threaten to leave law enforcement without large amounts of useful information.

[23] United States v. Place, 462 U.S. 696 (1983)(drug sniffing dog's use of its nose on luggage is no search because it "discloses only the presence or absence of…. A contraband item" and "does not exposenoncontraband items that otherwise would remain hidden from public view").

[24] Ciraolo, 476 U.S. at 209 (1986).

One exception to the trend away from property protection is the home. The Supreme Court recently overturned a Ninth Circuit decision allowing law enforcement to introduce evidence from a search initially undertaken because thermal imaging equipment had helped establish that marijuana was being grown in a home.[25] The court reasoned that the information obtained by law enforcement through the use of thermal imaging was equivalent to what could have been obtained with a more invasive search. Instead of viewing this similarity in information rendered as an argument in favor of the use of thermal imaging, the court viewed it as a problem: it could not imagine how to draw a principled line between the limited information disclosed by thermal imaging and the far more detailed information that could be disclosed by more sophisticated technologies.[26] The simple solution was to require a warrant where this technology was directed at the home and not in general public use.[27]

Beyond the police criminal investigation context, courts often apply different standards when interpreting Fourth Amendment requirements. Courts generally do not assume that the Fourth Amendment should restrain criminal and national security investigations in the same manner. On the contrary: national security interests may sometimes justify even warrantless electronic surveillance.[28] The doctrine also holds that many inspections and regulatory investigations do not count as searches. Investigators may deploy technology without it constituting a search in some situations without a warrant where exposure to the technology is a condition of some privilege, such as boarding a commercial flight.[29] Even where both common sense and court decisions

---

[25] Kyllo, 121 S.Ct. at 2028.

[26] Of course, even if the use of the thermal imaging technology in Kyllo is viewed as a search and requires probable cause, it may still be deployed by law enforcement subject to certain conditions. A valid warrant issued by a neutral magistrate pursuant to some showing of probable cause would make the technology's use possible – which might be useful to the government if it wants to gather information about a suspect's activities without being detected in order to prevent a terrorist attack.

[27] *See*, e,g,. Payton v. New York, 445 U.S. 573, 589 (1980)("The Fourth Amendment protects the individual's privacy in a variety of settings. In none is the zone of individual privacy more clearly defined than when bounded by the unambiguous physical dimensions of an individual's home"). As the court noted in Ciraolo, changes in the diffusion of technology might change the court's analysis of whether a law enforcement procedure is a search. *See* Ciraolo, 476 U.S. at 209 (1986).

[28] *See* United States v. United States Dist. Court [Keith], 407 U.S. 297, 315 (1972)(national security interests may justify warrantless electronic surveillance despite a citizen's right to privacy and to free expression).

[29] *Cf.* Camara v. Municipal Court of the City and County of San Francisco, 387 U.S. 523 (1967)(imposing a lower probable cause test for regulatory inspections where there is (1) long history of acceptance of such

conclude that there is a search (for example, if a government supervisor searches an employee's desk), the standards permitting the search appear lower than in the police context.[30] Although this distinction between police and non-police searches therefore has technical significance in the legal doctrine, it should not be overblown. The core functions of the Fourth Amendment still seem to be about limiting the pervasive discretion of government (but perhaps in principle, of large impersonal entities) to absorb information about people. Thus, even if Transportation Department surveillance of passengers at airport terminals does not necessarily trigger the heightened doctrines regulating searches applicable to police investigating crimes, there might still be grounds – based on constitutional values -- for imposing statutory limits on such surveillance.

In short, where the government is acting less in a criminal investigation capacity and more in a regulatory or preventive capacity, it is easier to conduct a search and comply with the requirements of Fourth Amendment doctrine. The search just needs to be reasonable in light of the totality of the circumstances. The more lax standards to which government search conduct is subject where the objective is regulation rather than traditional criminal enforcement do not imply that government regulatory conduct is less intrusive or problematic. Instead, the doctrine suggests that a greater concern with the interactions that can be more obviously coercive – involving the encounter between police and the people they patrol. Yet in some cases, a regulatory-type search (or even a private sector search) can be just as invasive and also lead to people being judged out of context, resulting in coercive consequences including the loss of a job, or the denial of access to commercial air travel. The Fourth Amendment's formalistic distinction between police and regulation (and, for that matter, between government and private sector activity) should therefore not limit the imposition of some ethical constraints on preventive, regulatory activity or private sector activity.

Despite the much maligned imperfections of Fourth Amendment doctrine, that doctrine highlights a recurring concern with the government's power to snoop around, to go on fishing expeditions, to arbitrarily detain people, to confiscate property absent some

---

inspection; (2) public interest in abating all dangerous conditions including those not readily observable without inspection; and (3) inspection involves limited privacy invasion).

[30] The standard seems relatively low in practice. *See*, e.g., New Jersey v. T.L.O, 469 U.S. 325 (1985)(searches of students by public school officials); O'Connor v. Ortega, 480 U.S. 709 (1987)(searches of government employees by supervisors).

justification, or to snoop around with no reason.[31] Of course privacy is not a universally understood concept,[32] but it appears in principle to encompass the core "right to be left alone" rhetoric that's animated Fourth Amendment doctrine, especially since Katz. To be sure, it's not a unanimous view that Fourth Amendment doctrine should be most concerned with privacy,[33] or even that the practical effect of the doctrine, stripped of its stirring privacy-centered rhetoric, actually evinces a concern with privacy.[34] But it's virtually impossible to deny that the doctrine reflects an effort to frame Fourth Amendment protections in terms of privacy. The development of constitutional doctrine has often reflected an imperfect fit between commitments made in the Constitution and goals achieved,[35] so the doctrinal criticisms about imperfect privacy protection surely does not imply that the value of privacy bears no relationship to how judges have decided (and continue to decide) Fourth Amendment cases. Thus, it would seem that the question of just how much information a technology reveals to government ought to be relevant not only for technical analysis of Fourth Amendment doctrine, but also for protecting the underlying constitutional value of limiting the government's blanket access to information about individuals.

B. Privacy Concerns Reflected Beyond the Fourth Amendment

The Fourth Amendment is just one example of the constitutional system's aspiration to value privacy. Since before the famous Roe v. Wade case, constitutional

---

[31] Even well before the opinion in Katz -- the most direct articulation of privacy's importance to Fourth Amendment analysis – the Supreme Court had begun to intimate that privacy mattered. Olmstead v. United States, 277 U.S. at 438 (Holmes, J., dissenting)(noting that federal wiretapping in violation of state law is "dirty business," and declaring it "a less evil that some criminals should escape than that the government should play an ignoble part"). *See generally* Sherry F. Colb, *Innocence, Privacy, and Fourth Amendment Jurisprudence*, 96 COLUM. L. REV. 1456, 1466-67 (1996)(" If, for example, the Fourth Amendment requires that a police officer have probable cause and a warrant to perform a search, then the individual has the right to privacy against state searches to the extent that a police officer lacks either one").

[32] *See* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN L. REV. 1393, 1446 (2001)(supplying the following definition of informational privacy: "an individual's right to control the terms under which personal information… is acquired, disclosed, and used").

[33] *See* William J. Stuntz, *Response*, 93 MICH. L. REV. 1102 ("It is common ground in Fourth Amendment law and literature that the law should protect privacy, that its primary purpose should be to regulate what police officers can see and hear. I believe this view is mistaken…").

[34] *See* Louis Michael Seidman, *The Problems with Privacy's Problem*, 93 MICH. L. REV. 1079, 1081, 1087-92 (1995).

[35] Obvious examples are Supreme Court decisions allowing for the continuation of mal-apportionment and of segregation well after the Fourteenth Amendment

doctrine has provided some support for the argument that a generalized right to privacy should be inferred from the "penumbras" of the Bill of Rights.[36] It is now accepted that the right guarantees a minimum level of non-interference in, for example, a woman's decision to end a pregnancy or a couple's decision to use contraceptives.[37] While the notion of a generalized right to privacy has made an imprint on the law, it's not clear what is the limit (or even precisely what is the source) of this right.[38] Many state constitutions and statutes also protect a right of privacy.[39]

The existence of substantive privacy protections underscores the constitutional value of creating zones of individual autonomy for the exercise of fundamental rights. Even if the original design of an enforcement strategy using sensor technologies focuses on terrorism, the concern is that such technology might later be used to make it easier to enforce a law that might substantively interfere with privacy. This type of "slippery slope" concern is pervasive in civil liberties advocates' evaluation of the technologies, and is discussed further below.[40] Privacy also protects people from being judged out of context – on the basis of salacious details or suspicious activity that would seem less bizarre if its context were also considered.[41] Privacy also protects individual dignity and autonomy, in the sense that Roe v. Wade, for example, protects certain decisions central to individual identity from government interference. Such interference may seem unrelated to the deployment of preventive technologies. But pervasive deployment of preventive technologies might make it easier for the government to enforce some laws that might, in extreme cases, rise to a level that interferes with identity as much as the laws at issue in Roe would.[42] All of these concerns – reflected in both Fourth

---

[36] *See* Griswold v. State of Connecticut, 381 U.S. 479 (1965)(recognizing a right to sexual privacy in the "penumbras, formed by emanations" from the Bill of Rights).
[37] *See* Griswold, 381 U.S. at 479; Roe v. Wade, 410 U.S. 113 (1973),
[38] *See* Jed Rubenfeld, *The Right of Privacy*, 102 HARV. L. REV. 737 (1989).
[39] *See*, e.g., CAL CONST. Art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending… privacy); FLA CONST., art. I, §23 ("Every natural person has a right to be let alone and free from governmental intrusion into his private life except as otherwise provided herein"); *see generally* ROBERT ELLIS SMITH, COMPLICATION OF STATE AND FEDERAL PRIVACY LAWS: 1981 (1981).
[40] The Fifth Amendment's self-incrimination prohibition also underscores the Constitution's concern with privacy, though it is almost never at issue in the context of preventive technologies because the bulk of its protections apply to custodial interrogations.
[41] *See generally* JEFFREY ROSEN, THE UNWANTED GAZE (2001)
[42] *See* Bowers v. Hardwick, 478 U.S. 186 (1986)(upholding state sodomy laws). While preventive technology is not meant to assist in the enforcement of these laws, the government sometimes uses an

Amendment doctrine and the more generalized privacy protections – should inform the manner in which technologies are deployed. Nonetheless, in the absence of the slippery slope argument, none of these concerns underlying constitutional privacy doctrines imply that the technologies should be rejected, since some technologies, in principle may even enhance certain kinds of privacy protections. For example, algorithms designed to screen what the information that the government receives could conceivably limit what data government gets; reduction in clunky, imperfect profiling.[43]

Finally, it is worth noting that the concern over privacy is not only enshrined in the Constitution. It has also been treated as a fundamental human right. For example, the 1948 Universal Declaration of Human Rights requires signatories (including the United States) to adopt legislative and policy measures to protect against the arbitrary interference with privacy.[44] So too is privacy a concern – at least on paper – for most legal systems in the world.[45]

C. Freedom of Speech and Association

The Constitution guarantees individuals a substantial measure of freedom from restraints on speech and association. The First Amendment explicitly protects freedom of speech and the press only from abridgment by federal legislation, but in 1925 freedom of speech was recognized as a fundamental right protected by the Fourteenth Amendment against abridgment by the states.[46] While there is no specific mention of a right of association in the Constitution, since the mid-20th century the Supreme Court concluded

---

enforcement approach justified on one basis to pursue a different law enforcement objective. For example, the post-September 11 dragnet focused on foreigners of a certain profile led to immigration sanctions against violators that had no connection to terrorism. *Cf.* Whren v. United States, 517 U.S. 806 (1996)(constitutional reasonableness of a stop does not depend on the actual motivation of the officer involved).

[43] The government might have a difficult time committing to abide by the limits set through the algorithm, but at least in principle it's possible to limit this problem by allowing neutral third parties (or Congress) to audit law enforcement's use of such algorithms.

[44] UN GA Res. 217A (III) (1948). *See also* International Covenant on Civil and Political rights, UN GA Res. 2200A (XXI)(1966, entry into force 1976).

[45] A U.S. State Department survey conducted in 1995 revealed that 110 countries guaranteed the right to privacy in their constitutions in some fashion, even if remedies for violations were inadequate. *See* David Banisar, "U.S. State Department Reports Worldwide Privacy Abuses," http://www.privacy.org/pi/reports/1995_hranalysis.html, (February 22, 2002).

[46] *See* Gitlow v. New York, 168 U.S. 652 (1925).

that people also possess a right to engage in association for the advancement of beliefs and ideas.[47] Even when asserted against the government, these rights are not absolute.

In most scenarios describing the proposed use of the technologies under discussion, there is no direct restriction of speech or association. No one has proposed using sensor technology to detect people expressing notional support for Al-Quaeda's underlying goals and to punish them.[48] But whether pervasive deployment of the technologies under discussion would have a chilling effect on some form of expression is a separate issue.[49] To some degree any such effect would depend on the technology in question. For example, we might expect some chilling of speech to result from the deployment of an ill-advised sensor system that singles out individuals for additional inspection on the basis of what they say. Other technology applications – such as government use of biometric identification systems and targeted data analysis – would not appear especially likely to chill speech or associational freedoms, unless they were used to enforce substantive legal prohibitions that themselves chilled speech. It's not obvious that such use would result, but here again the slippery slope argument reappears to highlight the possibility that technology deployed for one reason would be used for another.[50]

While a chilling injury is easy to understand as a matter of logic, it is tremendously difficult to obtain standing for a purely chilling injury to speech and associational freedom interests.[51] So too is it difficult to know whether the specter of a chilling effect should lead to restrictions on technologies. It is obviously hard to measure any chilling effect.[52] The perceived threat to constitutional values might even spur

---

[47] *See* NAACP v. Alabama, 357 U.S. 449 (1958)("[I]t is beyond debate that freedom to engage in association for the advancement of beliefs and ideas is an inseparable aspect of the 'liberty' assured by the Due Process Clause of the Fourteenth Amendment…").

[48] Although it seems far-fetched to believe the federal government would punish people for expressing support for an organization (no matter how unpopular), the Supreme Court has upheld the constitutionality of laws punishing individuals for associating with organizations that advocate the overthrow of the U.S. government by force. *See infra* note 107 and accompanying text.

[49] *Cf.* Estes v. Texas, 381 U.S. 532, 545 (1965)(noting the high probability that the presence of cameras in a courtroom would influence juror behavior).

[50] Section IV addresses the slippery slope problem.

[51] *See* Laird v. Tatum, 408 U.S. 1 (1972); Meese v. Keene, 107 S.Ct. 1862 (1987), *but see* Kolender v. Lawson, 461 U.S. 352, 358 (1983)(concluding that a substantially imprecise criminal statute affecting speech is unconstitutionally overbroad because of its potential chilling effecton speech).

[52] Empirical studies of chilling effects have the benefit of providing a basis to differentiate among different law enforcement strategies, all of which might seem troubling beforehand but not all of have the feared

potentially targeted speech and association in the short term. None of this means that fears of chilled free speech and association are irrational. But neither are those fears, by themselves, a compelling justification to reject most preventive deployments of technology, except perhaps for pervasive electronic surveillance.

D. Due Process

Where the government affects an individual's interest in life, liberty, or property, it must ensure that those interests are protected by due process.[53] Modern due process does not establish substantive limits on permissible legislation, but instead focuses on the procedures the government uses to determine whether a person should be subject to a particular legal restriction or requirement.[54] When faced with a potential due process issue, courts first inquire if there is a protected interest of liberty and property (since life is almost never at issue). Most of the technologies discussed here do not obviously threaten such interests, though they might if used in conjunction with a troubling enforcement strategy that did threaten liberty. Even if someone prevailed in arguing that a technology impacted a liberty or a property interest, there would still be the matter of how much process is due. The doctrine provides for balancing between the interests of government and those of the individual, both of which are considered in the context of whether the procedures in question increase the accuracy of a government decision. A person would likely have a legitimate due process claim if detained without communication or contact with a lawyer exclusively on the basis of a profile generated by data collection and evaluation technologies.[55] A person might also have a claim if data

---

effects. The caveat is that it's difficult to control for separate factors affecting expression, such as the degree of public concern about law enforcement policy. Experimental findings help develop intuitions about how and when people might react to changes in laws or law enforcement policy. *SEE* SHOSHANA ZUBOFF, IN THE AGE OF THE SMART MACHINE: THE FUTURE OF WORK AND POWER 344-45 (1988)(explaining the phenomenon of "anticipatory conformity" among persons who believe they are the subject of observation). But in most cases, the very definition of an experiment makes it less contextual and more contrived, so findings should be interpreted cautiously.

[53] Mathews v. Eldridge, 424 U.S. 319 (1976).

[54] *See* Brock v. Roadway Express, Inc., 481 U.S. 252 (using Mathews test to decide rights of employer who was ordered by government to reinstate an employee while the latter's allegations of retaliatory discharge was pending).

[55] Even something far short of detention – such as summary dismissal from a job as a result of analysis of data collection and evaluation systems – can amount to interference with a protected liberty interest. *See* Goss v. Lopez, 419 U.S. 565 (1975). The person detained could also bring suit to vindicate rights under the Fourth Amendment .

collection and evaluation software profiled her as a likely terrorist and this automatically led to some legal detriment (such as the loss of a government job), though the Supreme Court has upheld the "posting" of persons suspected of an offense when there is no direct legal sanction.[56] To the extent that the concern is not that, for example, recognition technologies would be used to stop dangerous passengers from boarding planes, but to keep track of everyone's movements, we again confront the slippery slope problem – which I address below.

International treaties also require signatories to ensure a baseline level of due process, even if the precise content of the concept remains inherently shrouded in some ambiguity.[57] The relevance of these provisions would likely arise only in the more extreme situations, where the preventive technologies were used as a basis for administering severe sanctions affecting liberty and property interests that are in any event protected by domestic constitutional due process doctrine. As with traditional due process analysis, the legal problem would not arise because of the technology itself, but because of the government interference with liberty (or property) justified on the basis of the technology.

E. Controls on Private Sector Technology Deployment

Few of the doctrines discussed above have any direct effect on what the private sector does with prevention technology. The Constitution is a means of shaping government's architecture and power. The doctrine places some limits on the extent to which government can forego its obligation to comply with the Constitution by outsourcing responsibilities to the private sector and then permitting private actors to

---

[56] *Compare* Wisconsin v. Constantineau, 400 U.S. 433 (1971)(finding that a state summarily posting lists of "excessive" drinkers violated due process, where liquor stores were forbidden from selling alcohol to people included in the lists, *and* Paul v. Davis, 424 U.S. 693 (1976)(upholding the distribution of flyers listing plaintiff among "active shoplifters"). The Paul decision has been roundly criticized because of the court's analysis concluding that the plaintiff suffered no injury to any constitutionally protected liberty interest, despite the assertion that the posting had impaired his job opportunities and injured his reputation.

[57] *See* Universal Declaration of Human Rights, arts. 6-11, *supra*; International Covenant on Civil and Political Rights, arts. 9 and 14, *supra*. The European Convention on Human Rights encompasses due process-related concepts in its discussion of rights to "liberty and security," a "fair trial," and a bar on "punishment without law." European Convention on Human Rights, arts. 5, 6, and 7, *supra*.

violate constitutional protections.[58] But in general, entities that are not part of the government are not subject to constitutional constraints.[59]

Instead of regulating such behavior directly, the Constitution lets the legislature worry about it. The private sector ends up with a substantial degree of flexibility to deploy preventive technologies. For example, employers can monitor their employees' electronic mail traffic and Internet access with minimal legal restraints.[60] Such flexibility allows the private sector to experiment with cost-effective approaches to resolve security problems – assuming that the private sector's own unauthorized or inappropriate use of information is constrained.[61]

Notwithstanding the reasons to allow for private sector experimentation and the Constitution's lack of restraints on most of what the private sector does, it is not difficult to make a case that such activity should continue to be subject to statutory controls. As Fourth Amendment doctrine highlights, in both the regulatory/national security and the more traditional police investigation context, individuals' expectation of privacy is crucial to determining whether a particular enforcement strategy (i.e., bundle of law enforcement policy and technology) counts as a search. That expectation, in turn, depends on both the individual's subjective impressions and what society is willing to tolerate as reasonable. As some technological practices become more common, driven in part by private sector activity, both of those variables will likely lead to greater acceptance of a technology's use – which will make the doctrine even more amenable to the use of such technologies. This often criticized feature of the doctrine is one way that private sector decisions about screening and surveillance technology might eventually

---

[58] The right-creating provisions in the Constitution regulate only conduct that is "fairly attributable to the state." *See* Lugar v. Edmonson Oil, 457 U.S. 922 (1982).

[59] *Cf.* San Francisco Arts & Athletics, Inc. v. U.S. Olympic Committee, 483 U.S. 522 (1987)(holding that the U.S. Olympic Committee did not violate the First Amendment rights of the plaintiffs when it sought to prevent the use of the name "Gay Olympics," since the Olympic Committee is not part of the government).

[60] *See* Kevin Kopp, Comment, *Electronic Communications in the Workplace: E-mail Monitoring and the Right of Privacy*, 8 SETON HALL COST. L.J. 861, 862-63 n.3 (1998).

[61] *See*, e.g., Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510 (establishing broad restrictions on private sector interception or access to the contents of electronic communications); National Labor Relations Act, 29 U.S.C.A. § 15 (1935)(prohibiting, inter alia, employer surveillance of union activities).

lead courts to be more willing to allow law enforcement to gather evidence by using such technologies.[62]

Indeed, Congress has imposed such constraints repeatedly.[63] The focus of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights is not merely on preventing state interference with privacy, but also on preventing unlawful and arbitrary interference with privacy by "…natural or legal persons."[64] Private sector organizations sprawl across local and national borders. They control access to valuable privileges ranging from commercial air travel to the rental of cars to financial transactions. It makes sense for statutory guarantees of privacy, due process or anything from the private sector to reflect a balance between the interests of the users and those of the private sector in operating efficiently and providing security. The absence of such standards in the face of massive deployment of technologies would be troubling.[65]

III. PREVENTIVE TECHNOLOGIES EXAMINED

The preceding discussion highlights the importance of considering technologies in context. The evaluation of a technology depends on the institutional arrangement involved in the deployment of that technology, which sheds light on how the technology will be used, by whom, and with how much accountability. For example, it would be difficult to make a legal or ethical evaluation of data collection and analysis technology without considering how authorities will use the information. Moreover, not every enforcement strategy that yields valuable law enforcement information is equally disruptive to a person. This is another way of saying that different technologies should

---

[62] The Supreme Court and its members have often recognized the circularity of the reliance on reasonable expectations of privacy, but still cling to the approach. *See*, e.g., United States v. White, 401 U.S. 745, 786 (1971)(Harlan, J., dissenting)("The analysis must, in my view; transcend the search for subjective expectations… [because] [o]ur expectations, and the risks we assume, are in large part reflections of laws that translate into rules the customs and values of the past and present"); Kyllo, 121 S.Ct. at 2028 (noting that the dissent's quarrel is not with the majority opinion but with the existing doctrine).

[63] *See*, e.g., Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510.

[64] Universal Declaration, article III, *supra*; International Covenant, article XXI, *supra*.

[65] But note that there is at least a possibility of a conflict between government restrictions on the use and revelation of private information and First Amendment doctrine. *See* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of the Right to Stop People from Speaking About You*, 52 STAN. L.R. 1049 (2000).

be evaluated differently, depending on a host of factors that can be conveniently grouped under the label "invasiveness." The label includes how much information the technology reveals and how physically or psychologically intrusive is the search (for example, sensing technologies that reveal the human form). Although this makes many sensing technologies appear more attractive compared to more invasive methods, it does not imply that any use of technology is low in invasiveness. For example, technology revealing the human form is probably psychologically invasive. Some sensing technologies can reveal a large amount of data about people. Even if the government's use of such technology were consistent with the doctrines discussed above, the technology may be overly invasive if it provides government (or perhaps even a private company) with far more data than what is necessary for defensible security purposes.[66]

This section surveys three major technology groups discussed at the conference – sensor technologies, identification and verification technologies, and data collection and evaluation technologies -- in light of the three constitutional values, then discusses specific applications of these technologies listed roughly according to their degree of invasiveness. Obviously, the categories are not completely separate. A sensor technology might be used in conjunction with identification or data evaluation systems, and even a specific technological application – such as biometric technology – can be an integral part of sensor or identification applications. But the categories generally serve to illustrate how preventive technologies might be used. Nor do the specific technology applications listed below exhaust all the ones available. They are meant to illustrate how different technology applications and types of deployment should be subject to different ethical constraints.

A. Sensor Technologies for Screening and Surveillance

Sensor technologies can help public and private sector bureaucracies recognize threats. The simplest technologies reveal even less information than the thermal imaging technology at issue in Kyllo, yielding only an indication of whether a particular substance

[66] The question is then whether the government can make a credible commitment not to use more than what it legitimately needs, and not to use what it needs improperly. One approach to narrowing the scope of what the government obtains from the deployment of advanced sensor or data collection and evaluation is to use an algorithm that filters out everything except what is permissible for the government to obtain.

such as an explosive is present in a piece of luggage or on a person's body.[67] More sophisticated sensor technologies such as long-range microphones or data scanners can acquire detailed voice and data streams.[68] Like the other technologies reviewed, sensor technologies have a host of useful applications in both the private sector and the government. The government's use of sensor technology for evidence gathering is subject to the requirements of the Fourth Amendment. Surely a remote sensing device scanning luggage for explosives (and only explosives) is equivalent to the drug sniffing dog that smell luggage without being considered to "search" that luggage.[69] The government's use of technology not widely available that are against the home or would pose a problem, as would use of sensor technology that violated individuals' reasonable expectation of privacy.

Explosive Detection: Explosive detection technology screens persons and physical objects to detect explosive substances. Some types of explosive detection technologies are already widely used at airports, but enhanced applications are on the horizon to improve the speed and accuracy of detection along the border and elsewhere.[70] Sensors geared to detect explosives, like any sensors designed to sniff out a very specific threat, are perhaps the paradigmatic example of technology that is acceptable in light of defensible legal and ethical constraints. Although no technology is perfect, it is relatively easy to evaluate the technology's effectiveness on the basis of whether it fulfills its specific objective.[71] If the technology only yields information about the presence of explosives, then its use is not considered a search under the Fourth Amendment.[72] Law enforcement can therefore use the technology to gather evidence admissible against a suspect at trial even without probable cause.

Note that the technology involved may be more complex than what would be necessary for more intrusive sensing, such as eavesdropping. For a sensor to detect a

---

[67] *See InVision Receives FAA Contract for Minimum of 54 and Up to 100 InVision CTX 5000 SP Explosive Detection Systems*, BUS WIRE, Dec. 26, 1996 (describing a contract for detection of explosives, such as detectors installed at airports that require physical swabs of exterior particles in luggage).
[68] Voice, visual, and data sensing technologies are growing in range and scope.
[69] *See* U.S. v. Place, 462 U.S. 696 (1983).
[70] *See* Lisa Rutherford, *Sensor Technologies*, presented at this conference.
[71] As with other applications, the less accurate the detection technology, the more important it is to build in procedural safeguards to reduce the damage done by false positives.
[72] *See* Place, 462 U.S. at 701.

specific threat it must do more than simply amplify something that can be perceived by an individual. Instead the sensor must recognize the particular characteristics of the threat with sufficient accuracy to warrant reliance. Yet this quality is what makes sensors of specific threats more attractive than technologies that provide government or the private sector with overbroad information that may have only limited relevance to prevention.

Unfortunately, the specificity of the focus of explosive detection technology is also what might place a limit on its ultimate usefulness for prevention purposes. By definition, explosive detection technologies (or other specific threat detection technologies) are hard-wired to sense and detect specific things. If this were not the case, then the technology would begin to look more like active millimeter wave technology or data analysis (both discussed separately). If terrorists learn that some explosives are easily detected they might shift to others, or perhaps even to means that are not explosives at all. Nonetheless, some specific threats are compelling enough to try to block with detection technologies even if the result is some substitution from detectable threats to less detectable ones.

Eavesdropping and Data Sensing: In most instances, government wiretapping, eavesdropping, or the equivalent achieved with more advanced sensor technology violates the Fourth Amendment when it is undertaken without probable and it pierces the reasonable expectation of privacy people might have in a protected setting such as a private home or office.[73] Accordingly, electronic eavesdropping or wiretapping that violate individual expectations of privacy are authorized by statute only in limited circumstances.[74] Where sensor technology does not violate a reasonable expectation of privacy – as with the drug sniffing dog or an explosive – there is no search and therefore no probable cause requirement.

---

[73] A number of cases shed light on the constitutionality of Title III of the Omnibus Crime Control Act. *See*, e.g., Osborn v. United States, 385 U.S. 323 (1966)(upholding a judicially authorized use of an undercover agent with a concealed tape recorder); Katz v. United States, 389 U.S. 347 (1967)(limited eavesdropping is constitutional if a warrant is obtained first). *But see* Berger v. New York, 388 U.S. 41 (1967)(finding unconstitutional New York law that permitted installation of surveillance equipment for an extended period of time and permitting renewal without a showing of present probable cause for continuance of the eavesdrop).

[74] *See* Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C.A. §§ 2510-2520.

The rules relating to eavesdropping and wiretapping in Title III of the Omnibus Crime Control Act are designed partly to allay constitutional concerns, but those concerns certainly do not exhaust the reasons consider separate statutory restrictions to restrain the use of some sensor technology. Statutory restrictions already have a substantial effect on government and private sector use of information obtained through sensor technologies.[75] Indeed, the private sector's use of sensor technologies is subject only to statutory constraints. But statutory restrictions can be subject to change in light of perceived security interests. Recently, the USA Patriot Act (or USAPA) weakened some of the constraints on the federal government's electronic surveillance of voice and data communications.[76] The statutory limitations that remain underscore the importance of statutory restraints to complement the meager restrictions provided by the Constitution. But since those are subject to change, as they did under the USAPA, it is worth considering what the constraints should be on technologies that make it easier for authorities to engage in electronic surveillance.

Whereas explosive detection technology reveals a tiny slice of information obviously related to security, electronic surveillance can yield the details of intimate conversations that individuals meant to keep private. This is problematic, since a technology's invasiveness depends at least in part on the breadth of information that can be gathered. In Kyllo, the court was unable to see an obvious means of drawing a line between thermal imaging and other technologies that would reveal even more intimate details from the home. This led to a sort of prophylactic rule against sense-enhancing technologies directed at the home, because they might be invasive. In Place, the court so readily accepted the drug sniffing dog because of the limited information revealed by the dog.[77] Even if one can make a principled case for some level of electronic surveillance,[78]

---

[75] *Compare.* California v. Greenwood, 486 U.S. 35 (1999)(upholding the use of an electronic monitoring device attached to an automobile to keep track of its movements on a highway), and United States v. Karo, 468 U.S. 705 (1984)(holding that placing an electronic monitoring device inside a container to track whether the container remains inside the suspect's house is a search, requiring probable cause).

[76] *See* USA PATRIOT Act, Pub. L. 107-56 (2001), Sec. 218 (relaxing the standard for obtaining authority to engage in FISA surveillance, from one requiring that purpose of investigation to be obtaining foreign intelligence information to one requiring that such an objective be a "significant purpose").

[77] United States v. Place, 462 U.S. at 696.

[78] *See generally* Thomas R. McCarthy, *Don't Fear Carnivore: It Won't Devour Individual Privacy*, 66 MO. L. REV. 827 (2001)(making a principled case in favor of targeted surveillance of electronic communication by law enforcement).

any such activity cries out for strong limits on what the authorities (in both public and private sector) do, when they do it, and for what reason. Because those constraints are difficult to police without information that is likely to be kept secret (to make the surveillance more useful), this is an area that merits aggressive efforts by outside interest groups to constrain government activity, especially where the targets of surveillance may be politically powerless and unpopular groups.

Active and Passive Millimeter Wave Technology Used to Screen Individuals: This technology, sometimes referred to as a "see through x-ray," allows authorities to scan individuals and objects more effectively than conventional x-rays to pick out a host of threats.[79] The prevention case for such technology is strong, because it is more flexible than explosive detection technologies and similar applications hard-wired to pick up only one threat. Admittedly, individuals subjected to such enhanced x-ray scanning may be troubled because it currently provides the user with an approximation of a scanned individual's naked human figure. It seems difficult to characterize a technology that reveals the naked human form as anything other than invasive, but electronic filtering techniques can reduce the invasiveness of the image without taking away its utility for prevention. More advanced deployments of millimeter wave technology provide capabilities similar to the forward looking infrared technology discussed below.

Forward Looking Infrared Technology: Forward looking infrared technology (FLIT) involves a more sophisticated use of the principle behind the thermal imaging technology at issue in the Kyllo case.[80] This application uses sensors capable of detecting small variations in heat, giving law enforcement to obtain a limited "view" of the inside of a building where the walls are not substantially thick or where curtains are drawn to cover windows.[81] The technology works by sensing slight variations in heat emitted by different objects, yielding a rough image of what is inside a building. The user may then visually scan the image of the premises for objects that appear to be threatening or for the presence of individual persons.

---

[79] *See* G.J. Burton and G.P. Ohlke, *Exploitation of Millimeter Waves for Through-Wall Surveillance for Military Operations in Urban Terrain*, LAND FORCE TECHNICAL STAFF PROGRAM, www.rmc.ca/academic/gradrech/millimeter-e.pdf (March 3, 2002).

[80] Some deployments of active and passive millimeter wave technology provide substantially the same capability as forward looking infrared technology. *See Id.*

[81] *See generally* Scott J. Smith, *Thermal Surveillance and the Extraordinary Device Exception: Re-defining the Scope of the Katz Analysis*, 30 VAL. U. L. REV. 1071, 1079 (1996).

Under Kyllo, the use of FLIT technology for home surveillance must constitute a search, since the use of the far cruder thermal imaging system amounted to a search. Indeed, because FLIT technology is not widely deployed and it has the potential to reveal details that people have sought to conceal, its use by police may also be constrained even where the focus is not a home but a commercial building.[82] Nonetheless, the government might still be legally entitled to use FLIT technology without probable cause in situations that do not involve police investigation (i.e., to scan automobiles at an airport).[83] Moreover, private sector entities might use FLIT technology to scan the interior of hotel rooms or other buildings.

Beyond the constitutional constraints, the use of FLIT technology in either the public or private sector should be subject to substantial statutory restraints. In contrast to the deployment of AMWT technology to scan individuals, it is difficult to envision how FLIT technology could be outfitted with a filter to make the information revealed less invasive. Perhaps it might be possible to filter all the images through a computer algorithm that only picks out genuinely threatening objects, but such a filter would be difficult to design without rendering FLIT useless for terrorism prevention.

B. Systems for Verification and Screening, Including Identification Cards

In most cases, there is no inherent constitutional problem with the government's use of recognition and screening technologies, unless the technology is used to advance impermissible substantive goals. Even where the government uses recognition and screening technology, it's not likely to count as a search because the recognition and screening would happen based on information that could be viewed by anyone, i.e., the visage of a person approaching a door.[84] If recognition and screening technology were to reveal information that could not be obtained through public observation, the use of such technology might constitute a search depending on whether the target were, for example,

---

[82] Ciraolo, 476 U.S. at 213 (indicating that expectations of privacy and the pervasiveness of the deployed technology informs the court's analysis of whether a search has taken place under the Fourth Amendment)
[83] *See* Section II.a, *supra*.
[84] *See* Karo, 468 U.S. at 705.

an industrial complex versus a home.[85] Finally, individuals seeking access to protected physical or electronic locations may be required to consent to the application of verification or identification technologies. I discuss specific applications below.

Biometric Verification Systems: Biometrics involves the recognition of persons through automated measurements of their unique characteristics.[86] Specific biometric technologies work by recognizing, among other things, an individual's fingerprint, hand, iris, retina, and voice recognition. One application of for biometric technology is in verifying whether an individual should have access to a particular physical or electronic location. For example, a smart card can include information describing an individual's fingerprint, which can serve to authenticate the holder of the card as the person entitled to access the secure area of an airport, or particularly sensitive data. Obviously, verification systems can also work without cards, by storing individual biometric identification information centrally. While the central storage of biometric information might raise concerns of abuse and the slippery slope (discussed separately), it is difficult to attack the principle of using biometric identification to authenticate an individual about to be granted access to a restricted location.

Biometric or Other Electronic Identification Systems: Whereas verification systems aim to authenticate an individual to establish authority to access some location, identification (or "recognition") evaluates a biometric sample of a person and compares it to a large set of individuals believed to be dangerous or suspicious.[87] This implies that a central database contains some set of records of the biometric information of the individuals that are being sought. Presumably, identification systems fulfill this function of detecting sought-after individuals (whether because they are known to be dangerous or simply believed to be suspicious), while also being suitable for authentication tasks. Thus, a system of biometric identification for access to restricted areas at airports could serve to verify that individuals accessing the restricted areas are authorized, but also to

---

[85] *Compare* Dow Chemical Co. v. United States, 476 U.S. 227 (1986)(finding enhanced aerial photography of an industrial complex not to be a search); Kyllo, 121 S.Ct. 2038 (2001)(concluding that thermal imaging of a home without a warrant constitutes a search).

[86] *See* Paul Skokowski, *Can Biometrics Defeat Terror,* presented at this conference (March 2002); *Electronic Benefits Transfer: Use of Biometrics to Deter Fraud in the Nationwide EBT Program*, GAO Report No. OSI-95-20 25-7 (September 1995).

[87] *See* Skokowski, *supra*.

monitor whether individuals considered suspicious (whose biometric information is known) have sought access.

Biometric identification can be used for specialized tasks such as the provision of airport security. Beyond this, biometric identification can form the core of a nationwide identification system.[88] The legal basis for the system could reflect one of three approaches. The most radical and invasive approach involves passage of a federal statute establishing pervasive requirement to make documentary or biometric identification available to authorities upon request. A second approach would involve the promulgation of federal statutory provisions requiring the use of reliable identification before individuals are permitted to engage in certain activities (such as opening a bank account or boarding a commercial flight). Finally, the national identification system could consist of private sector requirements for reliable identification imposed voluntarily. Private sector third parties could offer secure documents and biometric applications, while a federal statute provides a limited safe harbor from liability (though not from improper disclosure of information) and preempts any contrary state law.

Different approaches to a nationwide identification program merit different legal and ethical constraints. Opponents of national identification cards and biometric identification tend to focus on the first or second alternative. They tend not to argue that there is a right to a fake identity, but rather that a pervasive system might imbue government authorities with too much power to engage in pervasive enforcement or might degenerate into a system that squelches privacy. The pervasive enforcement problem is a substantial one, but only if an identification system requires people to carry around a specific document or to stop on command for a biometric inspection.[89] In contrast, more moderate private approaches might require the use of a national identification card with tamper-proof features or a biometric identifier to complete a particular transaction that could be fairly described as voluntary, such as getting on a

---

[88] *Id.*

[89] Some advocates of national identification propose just such a system. *See* AMITAI ETZIONI, THE LIMITS OF PRIVACY 113 (1999)("...all citizens (or residents) are required to carry this generic identification with them at all times... [and] presenting such indentification is required even when there is no specific evidence that a crime has been committed...").

commercial flight or opening a bank account.[90] The problem with the more ambitious approach is that police discretion can always be abused. If people were required to submit to inspection of identification documents or biometric identifies on command (i.e., on the street, at an airport terminal, at work, and so on), then police discretion over individuals would expand to the point that it might eviscerate the remaining Fourth Amendment probable cause requirements for most searches. Law enforcement would have authority to stop and check for identification documents in order to enforce the requirements, and the decision to stop someone would subject that person to some risk of search or seizure at the discretion of the police officer.[91]

Of course, even though there's no right to a fake identity, there is some inherent value in privacy, which might be undermined under a pervasive identification scheme yielding information housed in a central repository, unless there are controls on government use of that information. Though it's possible in principle to design a system of identification cards and biometric identification that does not end up allowing pervasive enforcement discretion, the cards and related approaches are most often decried because of the ubiquitous slippery slope problem (addressed below), which makes sense given that virtually all reasonable proposals for their use involve improvements in the enforcement of existing laws, rather than the implementation of drastic new prohibitions.[92] Even if one is persuaded by the arguments in favor of at least a national voluntary identification system, it is still particularly important to prevent abuse of biometric information. Biometric information is particularly sensitive because most of the biometric identifiers considered reliable – such as fingerprints – do not change materially over the course of an individual's life.

---

[90] Just where the line is between "voluntary" transactions and necessary ones is a difficult one to ascertain, but advocates of the more measured voluntary approach certainly do not imply that identification should be necessary in order to eat and breathe.

[91] *Cf.* Terry v. Ohio, 392 U.S. 1 (1968)(establishing the authority of law enforcement to frisk and partially search someone incident to a stop); Whren, 517 U.S. at 810 (establishing the permissibility of essentially pretextual stops and arrests).

[92] The one exception to this pattern might be immigration enforcement, which could become far more pervasive if the use of identification cards of biometric identifies were to proliferate, even in the absence of new substantive prohibitions. Such pervasive enforcement might be viewed as advancing the rule of law, but it could also fuel the view that sanctions for immigration offenses are unduly harsh. To the extent that sanctions are designed to "price" an offense, the appropriate level of a sanction depends on how pervasively the laws are enforced.

Facial Recognition Technology Deployed to Monitor Public Places: Facial recognition technology is a specific kind of biometric identification that can be used even where an individual in a public setting has not submitted to an inspection. Some law enforcement authorities and other government entities have undertaken experiments with facial recognition technology, enticed in part because the face currently is the only biometric feature that can be viewed from a distance. Presumably, the theory justifying such deployment is that through such technology, authorities are able to spot individuals believed to be suspicious (or perhaps known to be dangerous) in public places. But so far, the results of such experimental deployments have been underwhelming.[93]

At this point, wide-scale implementation of facial recognition technology is problematic. The technology's accuracy limitation is the first reason why such deployment is troubling: false positives could subject innocent individuals to detriment, and authorities would obtain little (if any) benefit over the use of existing strategies. Even if the accuracy problem were entirely remedied, the question would arise whether government could make a credible commitment not to use the technology to keep track of the movements of any person (or between) public places. Government restrictions on movement may run afoul of due process protections.[94] Nonetheless, widespread deployment of facial recognition technology could lower government's cost in tracking individuals, which can help government enforce laws that are substantively controversial.[95] Still, it's worth considering whether facial recognition technology can be rescued from the slippery slope because the technology might have some legitimate uses if the accuracy problem is solved and the slippery slope problem is addressed appropriately. For example, facial recognition technology can help police find suspects believed to be targeting a particular physical location such as an airport or a sports stadium.

---

[93] *See* American Civil Liberties Union, *Drawing a Blank: Tampa Police Records Reveal poor Perofrmance of Face-Recognition Technology*, www.aclu.org/news/2001/ n010302a.html (January 3, 2002).

[94] See, e.g., Qutb v. Strauss, 11 F.3d 488, 492, 496 (5th Cir. 1993) (assuming freedom of movement to be fundamental right and holding that ordinance satisfied strict scrutiny); Bykofsky v. Borough of Middletown, 401 F. Supp. 1242, 1248 (M.D. Pa. 1975) (considering plaintiffs' claim that restriction of freedom of movement constitutes violation of substantive due process rights), aff'd, 535 F.2d 1245 (3d Cir. 1976).

[95] *See infra* note 120 and accompanying text.

C. Data Collection, Evaluation, and Transmission Technologies

As with sensor and identification technologies, data collection and analysis technologies used by the government are not inherently offensive to the Constitution. Indeed, the government already finds regular uses for data collection and analysis technology.[96] But these and other uses should be subject to legal and ethical constraints.

Data Collection and Evaluation for Verification Purposes: Just as biometric identifiers can help ensure that only authorized persons have access to protected areas, so too can the collection of data, either through explicit queries (i.e., request for a mother's maiden name) or through evaluation of data submitted automatically from a smart card or an Internet access program. In principle, it is not difficult to defend technologies that collect data to authenticate whether an individual should have access to a protected area. Note that verification does not require data collected for verification purposes to be stored in some central location. For example, a card could include information on a person's social security number that is compared to data provided by an individual. If data are stored in a central location, the data should be safeguarded against unauthorized disclosure and slippery slope problems (discussed below) to prevent identity theft[97] or invasive privacy intrusions.

Selective Analysis of Unusual Patterns for Prevention and Investigation: Individuals and organizations generate vast amounts of data, some of which may be useful to analyze for preventive purposes. Government and private sector authorities already engage in such analysis. Airlines share information with the U.S. Customs Service about arriving passengers whose itineraries or ticket purchases justify additional scrutiny.[98] The Treasury Department analyzes millions of currency transaction reports each year to decide where to focus scarce investigative resources in combating money laundering. Specialized data analysis applications make it easier and more effective

---

[96] Examples of government use of data transmission and analysis technologies: the Financial Crimes Enforcement Network's FinCEN Artificial Intelligence System, analyzing currency transaction records and publicly available records to develop profiles of particularly suspicious transaction patterns; the U.S. Customs Service's use of advance passenger information voluntarily provided by airlines to pre-screen passengers and determine which might demand closer scrutiny when arriving at a U.S. port of entry.

[97] *See* U.S. Department of the Treasury, *Identity Theft Strategy* (1999).

[98] The U.S. Customs Service recently sought to persuade the few international airlines that did not currently provide advance passenger information to do so, indicating that a refusal to do so would result in passenger processing delays for the non-cooperating airline's customers.

examine such data, and individuals already have some privacy protections where government uses databases to engage in such analysis.[99]

Although selective analysis may seem problematic because it gives rise to arbitrary investigative decisions by authorities, the rejection of this approach conceivably leaves authorities with even more discretion to focus on problematic, observable characteristics (or nothing at all) as a basis for decisions about whom to investigate or subject to further inspection. As with other prevention technologies, selective analysis involves a paradox of sorts. It is less invasive than full content surveillance, because (by definition) only a narrow slice of information is the subject of law enforcement attention (i.e., financial transactions, airline tickets, visa applications, or firearms purchases, for example). Nonetheless, selective analysis must be used with caution because of the possibility that people will be judged out of context. Moreover, since the purpose of analysis is to focus investigative or inspection resources and not to ascertain guilt, individuals should not be subject to sanctions on the basis of a triggered profile. Finally, selective analysis raises the vexing slippery slope problem because, among other scenarios, selective analysis could degenerate into larger-scale centralization of data, in which case constraining the government and private sector organizations from improper use is even more difficult.

Large-Scale Centralization of Data for View and Data Mining: Whereas selective analysis involves a focus on limited types of information, large-scale centralization of data permits data mining across a vast array of types of information.[100] Just what information turns out to be effective in preventing terrorism is not always clear ahead of time, which is why data analysis technology is critical.[101] The federal government is currently prohibited from most applications involving large-scale centralization of data, but the restrictions do not apply to the merging of publicly-

[99] The Privacy Act of 1974, 5 U.S.C. § 552 et seq., extends database privacy rights to records kept at all government agencies. Under the terms of the statute, citizens are allowed to view any files kept on them by any agency – except where national security is at issue. Disclosure of the data to other agencies or third parties is restricted.

[100] Both public and private sector entities are developing link analysis and data mining technologies capable of analyzing vast amounts of data. For example, Defense Advanced Research Projects Agency (DARPA) is currently developing an application to evaluate the threat posed by different terrorist threats.

[101] A large number of data mining applications are used commonly in the private sector for marketing purposes.

available information, and existing statutory restraints are always subject to change.[102] Conceivably, such centralization could include information gathered through the sensor and identification/verification technologies discussed above. If government and the private sector use more information to mine data, they are less likely judge individuals out of context – even if due process protections are as essential as they are in the context of selective analysis.[103]

Nonetheless, authorities evaluating technology deployment should consider the civil liberties concerns that would arise if profiling and data mining technologies were used pervasively enough to create a regime where nearly everyone were constantly categorized on the basis of past behavior or probability of offending. Such pervasive categorization – especially when coupled with recognition and screening technology, could in principle begin to offend the concept of being treated on an equal basis in a liberal society.[104] But this concern should not be overblown, for it depends on what information is being collected and how the government is using it. Note in particular that the idea that there's a problem if people are categorized on the basis of past behavior or probability of future offense implies that there is some government response to the categorization. It is that response that could be most troubling. For example, if data

---

[102] The Computer Matching and Privacy Protection Act of 1988, 18 U.S.C. § 2701, explicitly bars the interagency merging of databases and information. Nonetheless, the statute is subject to a host of exceptions such as one providing for a national program to detect parents not meeting child support obligations. 42 U.S.C. § 653.

[103] Though selective analysis is more likely to raise problems of judging persons out of context, even data mining involving access to broader information is likely to yield false positives – such as airline passengers that are considered especially risky on the basis of multiple types of information. Forcing a person so identified to sustain a detriment beyond some additional inspection or investigation is offensive to the due process values that underlie our Constitution and legal system.

[104] William Safire offered such an argument in a recent critique of the D.C. Police's effort to expand surveillance, recognition, and screening throughout the District of Columbia:

> Digital images of the captured faces can be flashed around the world in an instant on the Internet. Married to face-recognition technology and tied in to public and private agencies around the world, an electronic library of hundreds of millions of faces will be created. Terrorists and criminals – as well as unhappy spouses, runaway teens, hermits, and other law-abiding people who want to drop out of society for a while – will have no way to get a fresh start.

William Safire, The Great Unwatched, New York Times (February 18, 2002), http://www.nytimes.com/2002/02/18/opinion/18SAFI.htm (accessed February 18, 2002). As with many slippery slope arguments, Safire's is potentially chilling, but not necessarily an accurate description of the chain of causality through which a monitoring system of 40 videocameras at public monuments and 200 at public schools becomes a panopticon linked to data collection and evaluation systems making privacy obsolete.

collection and evaluation technologies were used to obtain profiles of all airline passengers and the ones with excessively high profiles were categorically not allowed to fly, then Rosen's concern about categorization would be entirely valid. In short, the extent to which data collection and related technologies raise fundamental problems that offend the liberal state depend not on the fact of data collection and analysis, but on the consequences that follow from this analysis. Moreover, the large-scale centralization of data makes it potentially more difficult to prevent the government from using data to enforce laws that are unrelated to terrorism and more substantively controversial, such as criminal copyright infringement. The vast storehouse of centralized information could be an almost irresistible treasure trove for some government and private sector employees – a problem only partially allayed through the use of filtering algorithms that only allow authorities to see the information that triggers some profile of suspicion. Data centralization is therefore deeply problematic without approaches to solve the recurring slippery slope problem, which is the subject of the next section.

In short, the deployments of preventive technology currently envisioned at this conference do not offend the Constitution directly (although there are some outer limits, particularly involving criminal evidence gathering from home surveillance or from the use of radical new technologies). The question of whether a technology offends the Constitution or the constitutional values described above ends up depending substantially on the specific details of the technology and the ends for which it is used. For example, an explosive detection sensing technology with high accuracy is not a search in almost any context because it picks up only explosives, just as a drug-sniffing dog picks up only drugs. But any technology deployment pervasively implemented to gather large amounts of information poses larger ethical problems because of privacy intrusions that must be balanced against security interests, and because of the specter of the often-invoked slippery slope. I turn to both of these issues in the following section.

IV. DEVELOPING BALANCED LEGAL AND ETHICAL CONSTRAINTS

The review of specific technologies in light of the relevant constitutional values reveals two pervasive legal and ethical problems: balancing the costs and benefits of

technology deployment, and preventing the nightmarish slide down the slippery slope. Both problems are related: the inability to develop any useful framework to engage in balancing turns out to be one compelling argument in favor of rejecting a promising technology categorically because of the slippery slope (since presumably, if we can't do the balancing, then we won't be able to stop the slide down the slope). But it turns out that neither problem is necessarily as hopeless as it first looks.

A. Evaluating the Costs and Benefits of Deploying the Technology

Although the benefits of preventive technologies may be difficult to measure in practice, they are easy to imagine: deterrence of activity that creates risks, and detection of that activity where it is not deterred. Though it's harder to conceptualize the costs, it's not impossible. Privacy advocates make a convincing case that privacy has an inherent value by protecting dignity and autonomy, reducing the possibility of being judged out of context, and making it more difficult for government to make certain kinds of substantive laws. These costs include false positives arising from people being judged out of context.

Balancing of costs and benefits gets a bad name because it is sometimes viewed as implying quantification, yet obviously that critique implies some substantive vision of what is a "cost," and what is a "benefit." Obviously the whole exercise is meaningless if there's no content to those concepts, but it might also be a meaningless exercise if those concepts were so rigidly wound up around an ideal of quantification that would never be able to satisfy our conceptions of what should be valued. It's also true that just how to balance is difficult to establish and controversial – but it's the debate about how to do it that could prove instructive to legislators, public and private sector bureaucracies, and individual people. The constitutional values to which I've been referring may seem incommensurable, but as noted earlier much of constitutional doctrine involves balancing the interests of different individuals, or the interests of individuals against those of their government. Administrative agencies balance things that seem incommensurable all the time; albeit subject to a host of imperfections ranging from the cognitive limitations of agency staff to deliberately inefficient procedures embedded by legislative coalitions.[105]

[105] For example, Congress has often issued statutory directives requiring agencies to change their ways of making decisions to incorporate new procedures or to take account of new values and interests. For

Problems of security and civil liberties might seem far less suitable for balancing costs and benefits than environmental policy. Not so. Balancing is a defensible ethical premise because it allows decision-makers to weigh – at least in principle – the needs of different individuals and groups impacted by a particular technology.[106] Ironically, the Constitution is sometimes characterized as a series of inviolable proscriptions that that are anathema to the sort of balancing act I advocate. Obviously some of what the Constitution does is to prohibit things, a function reflected in the doctrine's resolution of clear-cut issues that require relatively little because they're settled by the constitutional text or by well-defined doctrinal precedent. Interpreting a more ambiguous provision of the Constitution, though, such as "due process," almost invariably requires some balancing of interests – even if courts might be loath to characterize such a process as one weighing costs and benefits.[107] So despite the apparent deontological structure of debates about constitutional rights, balancing actually finds support in multiple areas of constitutional doctrine, where courts weigh individual and collective interests when trying to determine if a particular law or policy violates the Constitution.[108] Even the seemingly categorical First Amendment, commanding that "Congress shall make no law…" abridging freedom of speech ends up being interpreted by the doctrine in a way that requires balancing.[109]

---

example, the National Environmental Policy Act of 1969, 42 U.S.C.A. §§ 4321-61 forced all federal agencies to balance their core objectives and the environmental impacts of major decisions. *See generally* JERRY MASHAW, GREED, CHAOS, AND GOVERNANCE 131-50 (1997)(describing how administrative agencies balance things that in principle seem incommensurate, in fields ranging from environmental protection to public benefits). For a more dyspeptic perspective on how well administrative agencies achieve this balance, *see* THEODORE LOWI, THE END OF LIBERALISM: IDEOLOGY, POLICY, AND THE CRISIS OF PUBLIC AUTHORITY (1969).

[106] *See* Richard B. Stewart, *The Reformation of American Administrative Law*, 88 HARV. L. REV. 1667 (1975)(articulating the importance of balancing costs and benefits faced by different groups when evaluating laws and policies). *But see* McNollgast, *Administrative Procedures as Instruments of Political Control*, 3 J. OF L. ECON & ORG. 243 (1987)(noting that administrative procedures may reflect differences in the political strength of interest groups).

[107] *See* Mathews v. Eldridge, 424 U.S. 319 (1976).

[108] Constitutional law doctrine involves balancing in a host of issue areas, including affirmative action; voting rights; due process analysis; and free speech.

[109] *See*, e.g., Branti v. Finkel, 445 U.S. 507 (1980)(while government employees generally have a First Amerndment right to freedom of political belief and affiliation, they can be fired for them if the hiring authority demonstrates that certain party affiliations are necessary for the effective performance of a job); Waters v. Churchill, 551 U.S. 661 (government employees may not be fired for disruptive speech in the workplace about issues of public concern unless the employee has reasonably investigated the facts of the alleged incident). While the "Congress shall make no law" part of the amendment gives a categorical command (subsequently to the states through the Fourteenth Amendment), parsing what is meant by

What further highlights the value of cost-benefit analysis is to consider the alternatives to many of the technology deployment strategies discussed here. For example, suppose all of the technologies that could possibly be viewed as invasive were rejected, including virtually everything discussed except perhaps explosive detection technologies. Presumably such an approach would obviate some of the slippery slope problems discussed below. But rejecting the deployment of some technologies will not make prevention any less urgent, which means we will probably have to accept alternative enforcement strategies, some of which may not be improvements over the technologies under discussion. The government would be left to rely on alternative strategies to promote prevention goals. Some of these strategies include the use of profiling and targeting individuals using imperfect, existing means; pervasive immigration enforcement, imperfect criminal finance enforcement (focusing primarily on physical currency aggregations and individuals known to police, but not others). A few problems tend to exist with these approaches. For example, profiling and pervasive immigration enforcement confer substantive discretion on law enforcement with potentially little accountability.[110] Sometimes that discretion is more likely to be subject to political checks (as is the case with local prosecutors and police departments subject to democratic pressure if the public is engaged and willing. But federal law enforcement is less subject to those constraints.[111] And in the wake of September 11, the public's concern with security makes it less likely that it will aggressively police rights and transgressions arising under existing enforcement strategies.

The technologies and enforcement strategies reviewed here can still yield mistakes – many of which can and should be measured as part of the continuing assessment of technology. Yet there is little basis to conclude that existing enforcement strategies are likely to be more accurate compared to existing technology in reducing

---

"abridging" is what requires balancing. *Cf.* McAuliffe v. City of New Bedford, 155 Mass. 216, 29 N.E. 517 (1892)("[t]he petitioner may have a constitutional right to talk politics, but he has no constitutional right to be a policeman").

[110] When law enforcement engage in profiling or targeting, they make a discretionary decision to exercise enforcement discretion on a subset of the total universe of possible investigative targets. The immigration context is one example of enforcement discretion

[111] William J. Stuntz, *The Uneasy Relationship Between Criminal Procedure and Criminal Justice*, 17 YALE L. J. 1, 3 (1997)(discussing the relative lack of political checks and accountability governing federal law enforcement).

false positives or identifying dangerous individuals. For example, while it is possible that data mining could lead to rigid "risk profiles" classifying some people on the basis of past (mis)deeds, rejecting data collection and data mining hardly implies that citizens are then treated equally. They are categorized on the basis of gross and imperfect criteria used consciously or unconsciously by law enforcement. Some of those categories and bases, imperfect as they may seem, are entirely condoned by law.[112] Other such categorizations are not legitimized – and may be condemned – by law, but it proves almost impossible to erase such questionable categories from the minds of law enforcement. For example, the law might prohibit some forms of profiling purely (or primarily) on the basis of race. Enforcing any prohibition against this when law enforcement officers still exercise discretion can be difficult, if not impossible.

The effectiveness of traditional imperfect profiling should not be automatically dismissed. But neither should the cost of concentrating on false positives on insular, discrete groups. Even if not all the costs and benefits of differing enforcement strategies can or should be quantified, they can be broken down into categories, differentiated by their nature (i.e., monetary cost, pressure against constitutional value, security cost, or what?), and also by who is impacted (everyone, no one, a very small number of people, politically powerless insular groups, or what?). The next thing to do is to consider whether, applying some defensible standard of balancing what could fairly be termed costs and benefits, existing enforcement strategies might be worse than those involving the use of preventive technology. Some of what police do today is almost certainly less effective and more problematic than what might be made possible by preventive technologies. Finally, although the balancing involved must in the end be normative, it can be usefully informed by some empirical investigation to see just what rights are chilled (on the one hand) and just how government and the private sector use preventive

---

[112] In a dissenting opinion in U.S. v. Sokolow, 490 U.S. 1 (1989), Justice Marshall criticized the police's penchant to claim different characteristics as being suspicious:

> Compare, e.g., U.S. v. Moore, 675 F.2d 802, 303 (6th Cir. 1982), cert. denied, 460 U.S. 1068 (1983)(suspect was first to deplane), with U.S. v. Mendenhall, 446 U.S. 544, 564 (1980)(last to deplane), with U.S. v. Buenaventura-Ariza, 615 F.2d 29, 31 (2d Cir. 1980)(deplaned in middle); U.S. v. Sullivan, 625 F.2d 9, 12 (4th Cir. 1980)(one-way ticket), with U.S. v. Craemer, 555 F.2d 594, 595 (6th Cir. 1977) (round-trip tickets)...

U.S. v. Sokolow, 490 U.S. 1, 13-14 (Marshall, J., dissenting).

technologies in practice (on the other hand). While many of these costs and benefits are not possible to measure quantitatively, empirical measurements can shed light on how people change their behavior (including speech and association behaviors) in response to the reality or perception that they are being observed. In addition, technology deployment should be coupled with evaluation strategies to inform deliberation about the technology's impact.

Admittedly, it is difficult to evaluate the costs and benefits of sensor, identification, and data collection technologies. Not all costs and benefits are easily quantifiable, or even quantifiable in principle. But the principle is less about quantification than about categorization. By setting out categories of costs and benefits, the evaluation process can identify potential beneficiaries and affected parties. Balancing therefore implies that the technology deployed must be reasonably effective and should incorporate due process protections to resolve instances where persons are inaccurately identified as suspicious. The degree of intrusion, moreover, should be proportionate to the level of risk from the threat that the technology seeks to address. Finally, where a technology is invasive, it should not be applied on the basis of indefinite, discriminatory categorizations that unevenly distribute the burdens of living with the technology.

B. Managing the Slippery Slope

Many of the arguments against deployments of preventive technologies are not, strictly speaking, purely legal arguments in the form of, for example, the use of technology X violates the Fourth Amendment. Instead they are partly political predictions with an if-then structure, commonly referred to as slippery slope arguments. You can recognize these a mile away: if we allow the government to do X, then it's akin to allowing the government to do Y, which in turn leads to the dreaded panopticon of constant omnipresent surveillance.[113] The implicit reason why X will lead to Y are not always spelled out, nor are they always the same reasons. As the discussion of speech

[113] Michel Foucault described the purpose of the "panopticon" in the following fashion: "to induce in the inmate a sense of conscious and permanent visibility that assures the automatic functioning of power." MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 201 (NEW YORK: VINTAGE, 1979). In other words, Foucault believed that pervasive surveillance would force the subject (i.e., inmate) to recognize the futility of challenging the rules because any transgression could be easily observed and punished.

and associational freedoms suggested, the slippery slope is a live tension that recurs in discussions of what is legal and what violates our constitutional values.

Principled civil liberties advocates might be willing to concede that some use of preventive technology (like explosive detection sensors at all airports, networked into a data collection and analysis system evaluating aggregate explosive threats) might represent an improvement over existing methods. But the slippery slope problem might still preclude their support of the approach because of a fear that the system just described would soon degenerate into an airport panopticon, and then into a pervasive one squelching privacy everywhere. Yet, because existing approaches are imperfect and the threats in question are real, in order to develop principled legal and ethical constraints we must unpack the slippery slope arguments to see if (and when) they hold as much water as seems to appear. Although slope arguments must be taken seriously they are neither as simple nor as inherently convincing as they might first appear.

To be sure, civil liberties advocates invoking the slippery slope have reason to do so. Some legal doctrine virtually builds in a slippery slope problem. The most obvious example is the Fourth Amendment's focus on the public's expectation of privacy as one element of the determination of what counts as a search. The more a preventive technology is used by the private sector, the more the public will come to accept it and reduce its expectation of privacy – which in turn makes it easier for the government to justify its use.[114] Even if doctrine did not explicitly incorporate changing public perceptions, deployments of preventive technology can habituate the public to a certain degree of surveillance and thus weaken political opposition to transgressions that might provoke consensus opposition at present (such as the use of sensor technology to obtain private information from homes).[115] Moreover, the easy availability of information can create a temptation for abuse that is impossible to resist. Richard Nixon's abuse of IRS records is just one cogent example.[116] Finally, civil liberties advocates concerned about

---

[114] *See* California v. Ciraolo, 476 U.S. 207, 213 (1986) (whether the use of a certain technology by law enforcement constitutes a search depends on changing public perceptions).

[115] For a discussion of the mechanics through which individual perceptions change, *see* D. KAHNEMAN, P. SLOVIC, AND A. TVERSKY, EDS. JUDGMENT UNDER UNCERTAINTY: HEURISTICS AND BIASES (1982)(discussing the cognitive strategies individuals use that give rise to changing their perceptions of prevailing conditions).

[116] *See* Joseph J. Darby, *Confidentiality and the Law of Taxation*, 46 AM. J. COMP. L. 577, 579 (1998)(discussing President Nixon's abuse of tax information to harass political opponents).

the slippery slope might argue that the public will have a hard time resisting increasing use of sensing, screening, and data transmission requirements once the technologies have a foot in the door, because some of the people most affected by these technologies (especially at first) will likely belong to unpopular categories (i.e., suspected terrorists, or undocumented immigrants).

If slippery slopes were always entirely certain to work their insidious magic, then we would have to reject some potentially attractive uses of preventive technology to avoid the unsavory consequences. If biometric verification controlling access to commercial airliners were certain to lead to government tracking of individual movements based on biometric identifiers, then even the innocuous verification scheme should elicit derision. What makes the issue more difficult is that it does not follow that slopes are slippery, and even if they are, it's not clear whether they're lined with slick oil or stubby sandpaper. For instance, courts are no strangers to the slippery slope. In response to actual or perceived instances of possible governmental abuse of vague standards, they impose prophylactic rules as they did in Kyllo. The court there had some sympathy for the argument that thermal imaging technology did not reveal intimate details from within the home but felt concerned that allowing the technology would not allow the court to restrain police from using ever more invasive technology.[117] Of course, courts cannot always be counted on to police slippery slopes – though sometimes it's hard to distinguish whether the court has simply reached a conclusion with which one disagrees or whether the court has failed to stop the executive branch from scoffing at rights guaranteed by the Constitution.[118]

---

[117] Kyllo, 121 S.Ct. at 2028.

[118] In June 1961, the Supreme Court issued three decisions, Communist Party of the United States v. Subversive Activities Control Board, 367 U.S. 1 (1961); Scales v. United States, 367 U.S. 203 (1961); and Noto v. United States, 367 U.S. 290 (1961), upholding national security laws and taking a decidedly narrow view of the First Amendment guarantee of freedom of association. All three cases involved federal legislation requiring the Communist Party and its members to register and disclose membership lists (and other information). In upholding the legislation, the Supreme Court noted that the legislative findings were not "unfounded and irrational imaginings." *Compare* United States v. Robel, 389 U.S. 258 (1967)(striking down a government loyalty-security program as an overbroad intrusion on the right of association). Moreover, even if a court sought to police the political branches' slide down the slippery slope, it's not clear that it would always be able to do so. *See* Robert A. Dahl, Decision-Making in a Democracy: The Supreme Court as a National Policy-Maker, 6 J. Pub. L. 279, 285 (1957)(noting that courts "are never for long out of line with the policy views dominant among the lawmaking majorities of the United States").

In any case, courts are not the only way to stop the degeneration of a preventive technology deployment into something more sinister. Just as courts undertake to police the slippery slope, so too do legislators and interested parties use structural and budgetary constraints limit the extent of slope problems. Interest groups may have both the power and incentive to police the slippery slope by making legislative changes, restricting appropriations, proposing sunset provisions, or simply focusing public attention on government conduct or private sector excess. The National Rifle Association vigorously polices law enforcement's use of investigative authority for firearms law violations, and the limited use of information on firearms purchases.[119] Banks have prevented the Bank Secrecy Act from turning into a blanket license for government access to financial information, despite Supreme Court decisions upholding the constitutionality of financial transaction reporting requirements.[120] Although tax information has occasionally been subject to unauthorized and inappropriate uses, the U.S. has built the world's most successful tax collection system in part because of taxpayers' expectations of confidentiality, protected by statutes.[121] Moreover, civil remedies may create limited government incentives to limit abuses.[122] Finally, technology's influence may not be purely detrimental on the slippery slope. Instead, technology itself can stock a toolkit of experimental approaches to making the vaunted slope less slippery (including, for example, algorithms that screen information and provide only limited chunks to the government; tracking systems to allow neutral third parties to evaluate how technologies are actually being used).

The point is not that all of these approaches will always halt the slippery slope, or even that any of them will. Instead they serve to illustrate that it is unconvincing to

---

[119] *See* WILLIAM J. VIZZARD, IN THE CROSS FIRE: A POLITICAL HISTORY OF THE BUREAU OF ALCOHOL, TOBACCO AND FIREARMS 92 (1997).

[120] *See*, e.g., Lopez v. First Union National Bank of Florida, 129 F.3d 1186 (1997)(discussing the limits of reporting requirements and safe harbors available under the Annunzio-Wylie Anti-Money Laundering Act, and concluding that bank's release of records in response to verbal instructions from federal authorities was not authorized).

[121] 26 U.S.C. § 7431(a)(l) provides that "[i]f any officer or employee of the United States knowingly, or by reason of negligence, discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103, such taxpayer may bring a civil action for damages against the United States in a district court of the United States."

[122] *But see* Daryl Levinson, Making Government Pay: Markets, Politics, and the Allocation of Constitutional Costs, 67 U. Chi. L. Rev. 345 (2000)(discussing limitations of civil damages as government action deterrents).

invoke the slippery slope as an argument for using law and ethics to achieve an outright ban the use of preventive technologies. It is unconvincing for several interrelated reasons. First, not all the technologies are equally invasive in the first place, so that not all of them provide the full panoply of information that might be so damaging to dignity or so likely to lead to judgment out of context. For example, although the use of evidence from thermal imaging of a home violates the Fourth Amendment (in the absence of a warrant), thermal imaging does not yield nearly as much information as sonic scanning of window panes (which could reveal private conversations), or Forward Looking Infrared Technology (which would reveal the layout and details inside a home). Second, not all legal doctrines have the sort of circularity built into Fourth Amendment analysis, where the sort of government evidence-gathering that is prohibited depends so heavily on what the public expects. In contrast, the indefinite seizure of a person who is not a foreigner purely on the basis of an algorithm's mined data, without any other means of establishing probable cause, is simply not legal. Lower courts may apply the doctrine wrong or fudge the determination of probable cause, but at least the doctrine is not explicitly *rigged* to incorporate changing public attitudes. Third, the enforcement policies bundled up with technologies can target different people and interests with differing degrees of political power. If bank customers and immigrants might both be subjected to data collection and analysis technology that could lead to false positives, it is likely banks will police government mistakes more aggressively than immigrants, who lack access to political recourse.[123] Of course, it's not always reasonable to expect politics to police the slope, especially in the immediate aftermath of September 11.[124]

---

[123] It's far from a pipe dream that invasive sensor technologies could be used to target politically powerless groups such as foreigners. Indeed, many of the legal strictures applying to eavesdropping conducted in the context of national security investigations explicitly require a focus on foreigners rather than nationals. *See generally* Susan Dente Ross, *In The Shadow of Terror: The Illusive First Amendment Rights of Aliens*, 6 COMM. L. & POL'Y 76, 120 (2001)("Evidence suggests the government singled out eight aliens for prosecution on the basis of their association with the Popular Front for the Liberation of Palestine"). Consider also that border searches do not require probable cause, and at least in some decisions the zone of U.S. territory associated with the border for law enforcement purposes stretches beyond an actual U.S. port of entry. *See* Almeida-Sanchez v. U.S. (1973)(upholding broad warrantless border inspections because of "national self protection").

[124] RICHARD E. NISBETT AND LEE ROSS, HUMAN INFERENCE: STRATEGIES AND SHORTCOMINGS OF SOCIAL JUDGMENT (1980) (noting how the recency of traumatic events can distort evaluations). The recency effect and similar features of human cognition militate in favor of sunset provisions that can be used to reevaluate the need for particular technology deployments.

By unpacking the different elements of the slippery slope argument so often used to argue in favor of ethical constraints on the deployment of preventive technologies, we can also disaggregate the evaluation of the technologies themselves – as well as the broader enforcement policies and laws that the technologies serve. As an illustration, consider the slippery slope problems involved where pervasive deployment of high-powered eavesdropping sensor technologies are used.[125] In contrast to screening and to data collection technologies, sensor technologies are explicitly designed to sense information that may not otherwise be easily observed. This tends to make sensor technologies more invasive, requiring greater legal and political resources to patrol private sector and government use of the information gathered.[126] Since Fourth Amendment doctrine is partly circular, pervasive use of the technology will increase the public's expectation that the technology is being used, which in turn will make it easier for the government to argue that it should survive Fourth Amendment scrutiny. Finally, if that the federal government decides to concentrate the use of sensor technology on foreigners, it's likely there will be less political pressure to constrain the technology's use. At a minimum, then, the deployment of technology just described could incorporate a number of safeguards, including provisions to allow for damage actions in case of private sector or government misuse of information gathered, sunset provisions to force some reevaluation of the technology's costs and benefits, and (in the case of the government) appropriations restraints to ensure the technology does not proliferate aimlessly. Legislators and outside observers should also consider if the technology targets a politically powerless group, such as foreigners or immigrants, but ironically the politically powerless status of such a group makes it less likely that legislators would be concerned in the first place.

---

[125] Assume for the purposes of this example the absence of statutory restrictions on private-sector eavesdropping and most government eavesdropping.

[126] It is also worth noting that courts have upheld the constitutionality of laws that impinge on freedom of association – which some find troubling – that might be more easily enforced through the pervasive use of sensor technology. For example, in Noto, 367 U.S. at 290, the Supreme Court upheld the Smith Act of 1940, as amended, codified at 18 U.S.C. § 2385 et seq., which among other things makes it a crime to associate with a group where the defendant knows that the aims of the group include the overthrow of the U.S. government or any of its subdivisions. Nonetheless, the court interpreted the statute (arguably to avoid a constitutional problem) and concluded that membership in an organization cannot be punished without a showing that the defendant actively affiliated with the organization, knowing of its illegal objectives, with the specific intent to further those objectives.

Obviously, not all use of sensor technology should be suspect. Explosive detection sensing does not raise the concerns that eavesdropping sensing does. Nor should we assume that screening and data collection technologies pose a minimal slippery slope problem. Rather, the point is that different constraints should be imposed on technologies depending on how invasive they are, who they target, and how feasible it is to design mechanisms that will restrain the technologies' abuse by government or private entities. The slippery slope poses a genuine threat of transgressions against constitutional doctrine and constitutional values; but the threat is not necessarily always an intractable one, nor does it affect all deployments of preventive technology equally. Much of this paper has sought to clarify the legal and ethical constraints that exist in principle. The challenge then becomes one of designing the institutional mechanisms for government and the private sector to commit to not abusing the technology infrastructure deployed for legitimate security purposes. It is only where it is impossible to design such a system for credible commitments should a technology be rejected on slippery slope grounds, and even then the issue should be revisited as we develop new strategies to police large bureaucracies.

V. CONCLUSION

McCarthyism and Japanese internment should remind us of the difficulties in policing the slippery slope and in balancing the costs and benefits of security and civil liberties. But the threat of terrorism compels us to take up those challenges when it comes to the deployment of preventive technology, because the alternatives are problematic. One alternative is to seriously question any feasibility of balancing analysis or restraints on slippery slopes and to press for the rejection of as much technology as possible. This approach is wrong, because it assumes that pressure to prevent terrorism is not going to stay constant, when there is every reason to believe that it will, or that existing methods are somehow always superior to approaches involving preventive technology. Another alternative is to focus on the magnitude of the threat, to view balancing and slope problems as overblown and to basically accept all technology that promises a preventive bonus, without imposing any constraints other than those provided by the letter of the constitutional doctrine. This is ridiculous, for it dismisses the danger

that society would not even be able to tell whether such a pervasive regime complies with the letter of constitutional doctrine (even though we'd know it doesn't comply with the spirit of that doctrine), and over time the pervasiveness of the deployment would itself change the nature of constitutional doctrine.

My observations about the two major problems in technology deployment – balancing and slippery slopes – may sound overly optimistic and trusting of government. To be sure, there is cause for concern about slippery slopes in preventive technology deployment, including doctrinal circularity, changing public perceptions that may water down future resistance, growing government temptation to use (and abuse) information gathering infrastructures, and political powerlessness of targeted groups. But slippery slopes are not always that slippery. Courts are sometimes able to police slippery slopes by demanding a record of why the government (for example) must do something, though admittedly this has failed on occasion. Dedicated interest groups working with legislators can use structural mechanisms to constrain the degeneration of one law or policy into another, as the National Rifle Association does in the context of firearms regulation, or banks have done in the context of money laundering enforcement. Legislators can also use sunset provisions and civil damage provisions against the government to police the proverbial line. Even without a dedicated single-issue interest group, legislators and government officials' own efforts to insulate information from abuse, as tax information has been, are not always futile (though admittedly they are not always effective). Finally, technology itself may be not only a source of slippery slopes but of leveling strategies like screening algorithms to limit what government actually gets, or tracking mechanisms to see how information has been used.

Some combinations of technology and bureaucratic power probably create more problems than they solve, so they should be rejected. But that's not a convincing argument to reject "technology" as a category of solutions. To reject technology simply because it raises amorphous liberty issues does not even do justice to the importance of those issues by leaving them so vaguely specified. That's as dangerous as justifying absolutely any deployment of technology – no matter how invasive -- on the basis of broad, unverifiable security concerns, while dismissing any contrary opinion as a mere invocation of "phantoms of lost liberty."